EXHIBIT 45

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,
Plaintiff,
v.
SOLARWINDS CORP. and TIMOTHY G. BROWN,
Defendants.
) Case No. 23-cv-9518-PAE

(30)(b)(6) STENOGRAPHIC VIDEOTAPED DEPOSITION OF SOLARWINDS CORPORATION BY ITS DESIGNEE JASON WALLACE BLISS
WEDNESDAY, OCTOBER 16, 2024

Reported by:
BRIDGET LOMBARDOZZI,
CSR, RMR, CRR, CLR
Job No. 241016BLO

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,
Plaintiff,
v.
SOLARWINDS CORP. and TIMOTHY G. BROWN,
Defendants.
) Case No. 23-cv-9518-PAE

Stenographic (30)(b)(6) videotaped deposition of SOLARWINDS CORP. by its designee JASON WALLACE BLISS, taken on behalf of Plaintiff, held at the offices of Latham & Watkins, 1271 Avenue of the Americas, Floor 33, New York, New York, commencing at 9:50 a.m. and ending at 7:47 p.m., on Wednesday, October 16, 2024, before Bridget Lombardozzi, Certified Shorthand Reporter, Certified Realtime Reporter, Registered Merit Reporter, and Notary Public of the states of New York and New Jersey, pursuant to notice.

APPEARANCES OF COUNSEL:

FOR THE PLAINTIFF:

SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, D.C. 20549-6553
Telephone: 202.551.4661
Email: todorj@sec.gov
carneyc@sec.gov
wardenk@sec.gov
stonel@sec.gov
BY: JOHN "JJ" TODOR, ESQUIRE
CHRISTOPHER CARNEY, ESQUIRE
KRISTEN M. WARDEN, ESQUIRE
LORY STONE, ESQUIRE (Remote)

A P P E A R A N C E S (Continued):

FOR THE DEFENDANTS:

LATHAM & WATKINS LLP
1271 Avenue of the Americas
New York, New York
Telephone: 212.906.1330
Email: serrin.turner@lw.com
maurice.baynard@lw.com
matthew.valenti@lw.com.
nicolas.luongo@lw.com
BY: SERRIN TURNER, ESQUIRE
MAURICE BAYNARD, ESQUIRE
MATTHEW VALENTI, ESQUIRE
NICOLAS LUONGO, ESQUIRE (Remote)

ALSO PRESENT:

JONATHAN JUAREZ, VIDEOGRAPHER
BECKY MELTON, In-house Counsel for SolarWinds

that I just mentioned sat within a hundred yards of each other in an Austin office, so there were a number of informal discussions and meetings that were conducted as well, whether through one-on-ones or the conversations in offices.

Q. Turning to the employees in the InfoSec group, during the 2018 to 2020 time frame, how many employees reported to Mr. Brown in that InfoSec group?

A. During, sorry, '18 to 2020?

Q. '18 to '20, yes.

A. Roughly around -- and you mean all -- the whole group, not just who reported to Tim?

Q. Correct.

A. Okay.

Q. The whole group.

A. So roughly around five to eight, I believe.

Q. And there's an executive, Eric Quitugua. Was he the -- I guess the principal deputy to Mr. Brown?

A. Yes. Eric -- Eric had been with the company as far back as 2015 and -- as an information security principal.

Q. Did Mr. Brown ever request to have more

personnel starting in -- okay.

First, was Mr. Brown hired sometime in the middle of 2017?

A. Yes.

Q. Did Mr. Brown ever request more people to have working for him between, let's say, that 2017 time frame and 2020?

A. I don't recall if he ever requested more people, but I'd be shocked if he never did because we all did. That's part of what a company does.

Q. And what was the annual budget for the information security group in this 2018 to 2020 time frame roughly?

A. It -- it changed, but I would say mid/high single digits to low double digits in the millions.

Q. Did that include salaries and technical resources they had available?

A. That would include salaries, bonus, cash compensation in general. It would include tools that would be allocated to that group. What it does not include, which is part of cybersecurity, are other elements in the business that would handle product security, for instance, or, as I

mentioned before, the legal department, who'd had a compliance function with cybersecurity. So that would only be his information security group budget.

MR. TURNER: I just want to note my objection to -- for the record, an objection to scope with respect to budget. I don't believe that was specified in the notice.

MR. TODOR: I'll just note that compensation is listed there in Topic 2.

MR. TURNER: That's fine, but I said budget. The witness was not specifically prepared to testify about specific budget numbers, so I just wanted to note that for the record.

BY MR. TODOR:

Q. In terms of locations of the employees in the InfoSec group, where were the employees located?

A. There were -- so Tim was in Austin. Eric was in Austin. There was an individual -- actually, Josh is in Austin. So mostly in Austin. There was an individual that came online in

Ireland. And I believe that was it.

Q. Okay. Was there a Tomas Sejna within the InfoSec group?

A. I don't have him in the Infosec group, as I recall. I believe Tomas Sejna either was prior to the relevant period or was in product security.

Q. Okay. And the individual in Ireland you referred to, is that Harry Griffiths?

A. That is.

Q. And did Josh Vanhoose -- is that the Josh you were referring to?

A. Correct.

Q. Any others that you're aware of?

A. There's a gentleman by the name of Ralph Greer. I don't know his location. And there was one other I can't recall.

Q. What were Kellie Pierce's duties as they related to cybersecurity?

A. Kellie was within the CIO office and she was a program manager. So Kellie's role was more to make sure that the trains were running on time, that notes were taken accordingly, that materials were produced. She wasn't a technical resource.

Q. Okay. In terms of the people with the -- providing the technical know-how for cybersecurity as they related to SolarWinds' cybersecurity group, would that include the information security group and would it include anyone else?

MR. TURNER: Object to form.

A. Can you clarify your question, what you mean by the technical --

Q. Okay. So you said Mrs. -- Ms. Pierce, for example, was not providing technical content.

Who were the people who were providing the technical content?

A. For?

Q. The cybersecurity --

A. For the information security group?

Q. -- issues in 2018 through 2020 time frame?

THE REPORTER: I'm sorry. You were speaking over one another. Can you please repeat that?

BY MR. TODOR:

Q. Okay. So you mentioned Kellie Pierce was not providing technical content. My question was, who were the people providing the technical

content within SolarWinds as they related to cybersecurity issues in the 2018 through 2020 time frame?

MR. TURNER: And object to form. I don't know exactly whether we're still talking about information security or product security or something else.

MR. TODOR: Okay.

BY MR. TODOR:

Q. So do you understand the question, sir?

A. I do.

There are numerous resources in groups, both in information security and beyond, within the company that would provide technical advice. As it relates to the internal IT environment, that would predominantly be InfoSec and folks within the CIO office like IT ops or business applications group.

And as it pertained to product security issues, there would be people in the engineering group with the product security team.

Q. And by "the engineering group," are you referring to Mr. Colquitt's group?

A. He would be one person in that group, but ultimately the engineering group --

engineering groups came together at Joe Kim and Steven Colquitt was one of the leaders within the Core-IT engineering team.

Q. And by "Core IT," you're referring to the difference between Core-IT and MSP, managed service provider, product lines?

A. Predominantly, yes. There was also a product line that goes by different names of cloud, application management, or app man, or cloud monitoring. And that was a very small business group that would have a closer relationship with Core-IT but was a separate group, yeah.

Q. So there were three general product lines: Core-IT, MSP, and cloud?

A. Correct.

Q. And each of those product line groups would report up to Mr. Kim?

A. Correct.

Q. And what were the cybersecurity duties that the product teams would have with respect to those products?

MR. TURNER: Object to form.

A. So when we were developing software and thinking about securing the product, most of the

responsible actions would be on the engineering teams. They would be advised by the information security team, but they were the responsible parties.

Also, as vulnerabilities were reported, that often was triaged by information security, but the work that had to be done would be on the engineering side of the house.

Q. What do you mean by "triaged by information security"?

A. As things were reported internally or externally, it was the initial intake method could vary. So it could come in through customer support, it could come in directly to information security group, but they would bring those together to monitor the activities of engineering.

Q. And turning back to the information security group, did Mr. Brown request an increase in the budget for the info -- information security group in the 2018 to 2020 time frame?

A. Yes.

Q. What -- what was he requesting an increase to do?

MR. TURNER: Object to form. I

MR. TURNER: Object to form.
A. If your question is whether there was a formal audit process on all of those answers to make sure there was accuracy throughout there, I don't recall a specific formal audit, but I know legal would look at answers provided to customers and ask questions for accuracy purposes. And I do know that our -- our mission was to provide accurate information to our customers.
Q. Okay. I'm just trying to understand processwise.
A. Right.
Q. There were questionnaire responses that had been generated at some point prior to the initial draft of the security statement being generated. A draft of the security statement was created largely using those preexisting questionnaire responses.
Was there an effort after that to go back and determine whether those original questionnaire responses were accurate?
MR. TURNER: Object to form.
A. When the security statement was pulled together leveraging that knowledge base and those items in there, I don't know if changes were made

in the initial draft, but the review process between Tim, between Rani, between legal was making sure that these statements were still accurate.
Q. How -- breaking that down, what was Mr. Brown's role in making sure that the technical statements were accurate in the security statement?
A. I think, as I previously said, he would review it. And what his processes were of reaching out to folks, I don't know that answer. But he was in a review to look at this document and be comfortable with this document.
Q. Okay. Do you have anything to add to Mr. Brown's deposition in terms of what steps he took to verify the information in the security statement?
A. I do not.
Q. And with respect to Ms. Johnson's review of the technical accuracy of the -- the information in the security statement, what was her role in that?
A. Similar to Tim's.
Q. Who at SolarWinds maintained this knowledge base that you're referring to in your

answers?
MR. TURNER: Object to scope.
A. I don't know if there was a single custodian, to use legal language, of this one document, but it's certainly something that was seen between Eric Quitugua, between legal, for instance.
Q. Was there a quality control process for this knowledge base information?
MR. TURNER: Object to scope and form.
A. Yes. As I mentioned before, we would go to the experts that could answer those questions to make sure we got the highest quality accurate information presented and legal was involved to varying degrees to look at it as well.
Q. Which individuals at SolarWinds were involved in this quality control?
A. Whoever was the expert on the question, depending on the question, and members of the legal team.
Q. Was there a -- a written process for it?
A. No. As I explained before, there was not a rigid process for this sort of activity.

Q. I turn your attention to the statements in the security statement under "Organizational Security." The second paragraph states "SolarWinds follows the NIST cybersecurity framework with layered security controls to help identify, prevent, detect, and respond to security incidents."
What information was relied upon to generate that statement?
MR. TURNER: The -- go ahead. I'm sorry. Go ahead.
A. This, as early as 2017, we were looking at the NIST cybersecurity framework as a voluntary framework we were using to help guide our cybersecurity program.
Q. When you say you were looking at it "as a voluntary framework," is that the same thing as you're saying you follow the NIST cybersecurity framework as it says in the security statement?
A. Yeah. I don't think following the NIST cybersecurity framework means much more than we used the framework as it was intended to be used in terms of measuring, identifying issues, assessing our overall cybersecurity program.

Q. What degree of control did Mr. Brown have over SolarWinds' cybersecurity practices as they relate to following the NIST cybersecurity framework?

MR. TURNER: Object to form.

A. I don't understand.

Q. Did Mr. Brown have the authority to say, yes, we're going to follow NIST cybersecurity framework or some other approach?

A. He certainly could have provided that input, yes.

Q. Who would have made the decision on that ultimately?

MR. TURNER: Object to form.

A. That level of decision probably would have been made from not just Tim in a vacuum, but it would have included Rani as well and perhaps even Joe.

Q. You say SolarWinds started looking, I think you said in your prior response, at the NIST cybersecurity framework in 2017.

At -- at some point did SolarWinds start having scorecards for its maturity level on this cybersecurity framework?

A. When you say "scorecard," what exactly

do you mean?

Q. So in the quarterly risk reviews and the security compliance quarterlies, there would be scorecards. We might see some of them later.

A. Yes.

Q. Why was that decision made and -- and did that reflect some -- let's answer that one first. Why was that decision made?

A. So the scorecard was a template or a format that presented the underlying NIST assessments. The decision was made to create that template or that visual because it provided distilled information at the level for the audience there, which in the QRRs were executives.

Q. Okay. Was SolarWinds tracking maturity levels on the NIST cybersecurity framework before it started having the scorecards on the presentations to the senior executives?

A. Yes.

Q. When did it start doing that?

A. I don't know a precise date, but I know that Eric Quitugua was looking at the NIST cybersecurity framework in early 2017.

Q. Was that an organizational decision that

Mr. Quitugua would be making that analysis or was that something Mr. Quitugua did on his own?

MR. TURNER: Object to form.

A. I'm not aware of the exact process there.

Q. Were there any action items as a result of maturity levels on the NIST cybersecurity framework within SolarWinds during the relevant time period as in you need to improve X area as a result of NIST cybersecurity maturity levels that were measured?

MR. TURNER: Object to form.

A. Are you saying did we adjust overall resources and activities with the scorecard or the underlying NIST framework assessment in response to those?

Q. Yes.

A. Yes. That's part of the purpose of the CSF, is to identify and assess your environment and look at where you have existing activities and to measure what is being done.

Q. What -- who at SolarWinds would be making that kind of decision?

A. I think it would be varied based on the materiality of those activities.

Q. I turn your attention later to the page 3 of the document where it says "Access Controls."

What, if any, control did Mr. Brown have over SolarWinds' cybersecurity practices that related to access controls as described in this paragraph?

A. Again, he would be a very important voice in advising on what's happening in the industry, how it's evolving, how we should evolve, and advising IT operations who, in this specific example, implemented role-based access controls.

Q. Looking to the next section on "Authentication and Authorization." And you can familiarize yourself with the section as you need to. My question will be similar.

What degree of control did Mr. Brown have over SolarWinds' cybersecurity practices as they relate to authentication and authorization as described in this section?

A. It's difficult to answer because the statements are very high level. For instance, we say "We require that authorized users be provisioned with unique account IDs." That is

addressed questions we were getting, the trust center came to be.
Q. I'm not asking you to get into technical details, but what were the other kinds of items that were included in the trust center other than the security statement?
MR. TURNER: Object to scope.
A. I don't recall without looking at it right now the other elements.
Q. Why was the security statement included in the trust center?
A. I don't know why it was included in the trust center other than it needed a place to land and maybe this was simplifying the website to have one place with various artifacts that might relate to each other.
Q. Okay. Did the items in the trust center all relate to security in some fashion?
A. I -- I don't know what else was out there.
MR. TURNER: Object to scope.
THE WITNESS: Sorry.
Q. Did -- was the trust center more prominent on the SolarWinds website than the security statement was prior to its inclusion in

the trust center?
MR. TURNER: Object to scope, form, foundation.
A. I don't know.
Q. Who at SolarWinds was responsible for deciding what content would be placed in the trust center?
MR. TURNER: Objection to scope and foundation.
A. I don't know.
Q. What was the process of approval of content to be placed in the trust center?
MR. TURNER: Same objection.
A. I don't know.
Q. Did Mr. Brown have any approval -- role in that process?
MR. TURNER: Same objection.
A. I don't know.
Q. Did SolarWinds ever direct customers to look at the trust center for any reason?
MR. TURNER: Objection to scope and foundation.
A. I don't have any specific knowledge that we did or didn't.
Q. Did SolarWinds ever direct investors to

look to the trust center?
A. I don't think so.
Q. Did SolarWinds ever direct investors to look to the security statement?
A. No.
Q. Turning your attention to Topic 7 of the deposition notice, which is "SolarWind's cybersecurity practices and policies during the relevant period as they relate to the topics discussed in the security statement, including, but not limited to" and there are five subcategories.
First, I'll ask about Topic 7.a, which is "whether and how SolarWinds followed the NIST cybersecurity framework."
First, I'll direct your attention to the security statement, number 5 under page 1, "Organizational Security," and to the second paragraph, first sentence, with the statement: "SolarWinds follows the NIST cybersecurity framework with layered security controls to help identify, prevent, detect and respond to security incidents."
Was this statement accurate for the 2018 to 2020 time frame insofar as SolarWinds is aware?

A. Yes.
Q. I think your previous answers might have touched on this, but did SolarWinds follow the NIST cybersecurity framework throughout the relevant period?
A. Yes.
Q. What criteria did SolarWinds use to determine whether it was following the NIST cybersecurity framework?
MR. TURNER: Objection to form.
A. So the framework is available for a team to identify and manage and assess its cybersecurity program and there are communications and documents and artifacts like the security scorecards that evidence that.
Q. Okay. Did SolarWinds ever apply NIST 800-53 as criteria to use in determining whether it was following the NIST cybersecurity framework?
MR. TURNER: Object to form.
A. I don't think I understand the question there.
Q. Did SolarWinds refer to the NIST 800-53 criteria to determine whether its cybersecurity

controls were sufficiently mature?
MR. TURNER: Object to form.
A. Not the way you're saying it, no.
Q. How did SolarWinds refer to the NIST 800-53 criteria?
A. So we would -- 800-53 is different from the cybersecurity framework in that the framework is exactly that. It's a framework that's utilized to identify SaaS and manage. There isn't like a one-size-fits-all solution, but it's meant for companies to utilize to continuously improve their program and to make sure that they're allocating resources appropriately.
800-53 is a set of specific controls that, as I know, are for heightened standards that are prescribed that you could go one by one to assess where you stand against those. They are not required and it is certainly not the intent of 800-53 for someone to meet all of those controls. But they are used as an informative reference for companies to utilize as another type of assessment on the cybersecurity programs.
Q. I direct your attention to Topic 7.b in the notice, which is "SolarWinds' access control practices and policies, including, but not limited

to, its 'least privilege necessary basis' practices and policies and virtual private network practices and policies."
And I'll turn your attention in the security statement to page 3, to the heading "Access Controls." I'll first ask you to review the paragraph for "Role Based Access." Let me know when you're ready.
A. I'm ready.
Q. Okay. And I direct your attention to the third sentence where it states "Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know/least privilege necessary basis."
To SolarWinds' knowledge, was this statement accurate for the relevant period, roughly 2018 through 2020?
A. It was.
Q. What -- how did SolarWinds determine that that statement was accurate for this time period?
MR. TURNER: Objection to form.
A. So there were multiple processes during the relevant period that related to access

controls and ensuring that those were implemented on a least privilege basis.
Q. What were the "multiple processes" you were referring to in your previous answer?
A. We had a process that utilized what's called a SARF, S-A-R-F, form that would establish access rights for individuals based on their role as they were both onboarded, as they changed roles within the company, as they were offboarded. That would be reviewed by the appropriate personnel.
We also bootstrapped that with user access reviews that were done on a quarterly basis to make sure that these access rights were being implemented appropriately. And the InfoSec team had a solution or tool they used that would notify them if access rights changed in certain ways.
Q. Okay. Were -- in the 2018 to 2020 time frame, were there any instances in which users had privileges that were set higher than they needed to be in terms of the least privilege necessary basis access policy?
MR. TURNER: Objection to form, foundation, scope.

A. Is your question were there rights granted to anyone beyond -- in this company beyond what was ideally prescribed?
Q. So it's -- was -- were there instances in which users had access that was broader than the policy stated they ought to have had?
A. I would -- I don't -- can't think of something specific right now, but I would say very likely there were isolated events of that. I'd be shocked if there were not isolated events of that.
Q. Was there ever a contemplation of changing the security statement in light of there having been incidents of that nature?
A. No, because it's simply saying that these access controls are set in a least privilege basis, which is what we had procedures in place to do. The fact that an isolated event might occur where somebody might have rights beyond what they should that would have been captured by user access reviews, is certainly not a significant thing to change that statement.
Q. What was your basis for the use of the word "isolated" in that answer?
A. So there are millions of rights that

products and the Orion improvement program."
And I direct your attention back to the security statement to the "Access Controls Authentication and Authorization" section. Oh, I'm sorry, this is the SDL section --
A. Okay.
Q. -- the "Software Development Life Cycle" section. Sorry about that. And I guess familiarize yourself and let me know when you're ready to discuss that section.
A. Okay. I'm ready.
Q. Okay. And I'll ask you about the statement in the third section. The third paragraph of the first -- third sentence of the first paragraph states "Security and security testing are implemented throughout the entire software development methodology."
To SolarWinds' knowledge, is this statement accurate for the 2018 to 2020 time frame?
A. Yes.
Q. Okay. How did SolarWinds determine that?
A. I'd refer you to Joe Kim and Steven Colquitt's testimony on this.

Q. Do you have anything to add to their testimony on this point?
A. I thought their testimony was more detailed than I'm going to be able to provide, but that is part of the agile methodology and the QA testing that's involved in that; that it's iterative and implemented throughout the software development life cycle.
Q. And I'll direct your attention to the first sentence of the second paragraph under "Software Development Life Cycle." It states "Our secure development life cycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments."
To SolarWinds' knowledge, was this statement accurate for the 2018 to 2020 time frame?
A. It was accurate.
Q. What's the basis for concluding that it was accurate?
A. I'd refer you to Joe Kim and Steven Colquitt's testimony on this, but there are artifacts that we have on vulnerability testing and regression testing and penetration testing and

product security assessments during that period for the products.
Q. Were there any changes to the secure development life cycle policies in the 2018 to 2020 life cycle in terms of making them more formalized?
A. There was an initiative that Steven Colquitt was running that was aimed at improving and utilizing new methods or new technologies, the overall development life cycle in that two-year period, yes.
Q. Okay. Was there any consideration of changing the statements in the security statement as they relate to the software development life cycle in light of that initiative?
A. No. What he was proposing would have been in addition to what's stated here and beyond what the security statement is saying.
Q. In your previous answer on whether the raw statement was accurate, you -- you stated "I'd refer you to Joe Kim and Steven Colquitt's testimony on this, but" it looks like you said "there are artifacts" or they are artifacts "that we have on vulnerability testing and regression testing and penetration testing and product

security assessments during that period for the products."
What did you mean by "artifacts"?
A. I meant there are documents, like penetration testing results, there are regression testing notes and results and vulnerability testing results that are in -- mostly in confluence within our environment with things that existed during this period of time that reflect that the development team was conducting these activities.
Q. Okay. Is "artifacts" like a -- a term with a specific meaning within SolarWinds?
A. No. It's a term that I use every now and then to just describe something that exists. You can replace it with "things" if you'd like.
Q. Okay. I had visions of digging up things.
A. Sorry. Didn't mean to get us on a tangent.
Q. Just trying to understand.
Turn your attention back to the response to the request for admission, please. I direct your attention to Request 41 on page 15. And you can take a look at it and familiarize yourself and

the user IDs and passwords sections of that user access process narrative document we've just been looking at?

A. So I think I said this earlier. That sentence in the security statement is basically just saying we have password policies that apply to our systems. That is not what the user access process narrative is saying. This is a more specific statement with respect to certain systems.

And so I don't -- I don't think -- and I think I said this. I don't think those two things are synonymous, is where I'm getting to.

Q. Okay. What is the nature of the difference in terms of what is meant by password policy in the security statement as opposed to this "User IDs and Passwords" section of the user access process narrative?

A. Again, I think this is just more specific about certain systems. I don't see that security statement representation there saying the same thing as this. Just because it uses the word "password" and "policy" doesn't make them the same.

Q. Looking through here on the user access

process narrative document, are there references or descriptions of the encryption requirements for the passwords?

(Pause)

A. I don't see any.

Q. Okay. So in -- in the security statement, there's the statement that passwords are "individually salted and hashed."

A. Correct.

Q. Is there some document that sets that forth as an internal policy apart from the security statement itself?

A. Again, as I mentioned earlier, the first sentence talks about unique account IDs, mostly. We're talking about Active Directory, this paragraph, right, our internal management system. And in Active Directory, those passwords are individually salted and hashed.

So is there a written policy on that? I'm not aware of one. Is there a policy on that? Yes, in Active Directory.

Q. Okay. Was there a password policy for some -- apart from user ID password requirements for maintaining passwords of an encrypted state?

MR. TURNER: Objection to form. You mean act -- Active Directory? You said "apart from user ID."

MR. TODOR: Yeah.

BY MR. TODOR:

Q. So looking back to the "Authentication and Authorization" statement of the security statement stating passwords are "individually salted and hashed," is that statement relating solely to Active Directory or is it referring to something else?

A. Well, I -- I believe that's referring to Active Directory because -- take an example. I can't force Westlaw to implement salting and hashing on the password that I set up on my user ID account. I only have control to the SolarWinds' accounts.

So that statement is nonsensical as it applies to systems that are third party outside of our control. It is very reasonable to think that is about our Active Directory accounts which SolarWinds controlled.

Q. Mm-hmm. About ready for our next topic. The Topic 8.a in our deposition notice, please. And Topic 8 is "SolarWinds' internal

evaluations of its cybersecurity practices, including, but not limited to," and seven subparts, the first of which is "SolarWinds' NIST 800-53/FedRAMP assessments, including, but not limited to, the June 2019, August 2019, and September 2019 assessments as reflected in documents" with Bates numbers that are listed there.

So, first, generally, are you familiar with SolarWinds's performance of NIST 800-53/FedRAMP assessments?

MR. TURNER: Objection to form.

A. I am familiar with an assessment. I'm not sure specifically if it's these without seeing them.

Q. What -- okay.

Why were the assessments that you're aware of performed?

A. So back to our conversation on business units. Core-IT, which was the flagship business unit and represented a majority of our business that had been with us since the beginning, had the Orion product, NPM, NCM, et cetera -- capital NPM, capital NCM, et cetera -- that had government

customers, both use U.S. federal and international government customers.

(Record notes Annie Gravelle is now present on Zoom.)

A. We acquired companies over time. And so I mentioned we acquired a couple of companies to create the MSP business unit.

In around 2015, we acquired a few small companies to jump start us with technology to deliver services in a SaaS deployment. S-a-a-S. That was our application management grouping or cloud grouping of products. Those products had a small number of customers and I don't recall there being government customers.

So with any acquisition, we would look to the product and say can we cross-sell that product to our customer base in Core-IT? which was a large, loyal customer base. And as we looked at the cloud products, the question became, what do we need to sell those products to our customer base of which some of that was government customers?

And the comment was, look, to sell a SaaS product to government, you'll need to invest in FedRAMP. And we understood FedRAMP was a long,

arduous, expensive initiative.

So we wanted a quick, cursory, preliminary review as to how much do we think this is going to cost us? How much effort needs to go into this? And we tasked that to our team that deals with SOC-2 and those types of certifications.

So this ended up with Kellie, who's a nontechnical person, more or less spitballing with what she knew about documents through SOC-2 and trying to understand what's the scope of activities we would need to do to obtain FedRAMP compliance with our cloud properties and how long would that roughly take.

Q. So let me take you back in your answer. I think you said you would task it "to our team that deals with SOC-2 and those types of certifications."

Who was on that team?

A. At that time -- again, SOC-2 is a very collaborative effort, but the program manager, who would make sure the trains of this was running on time, was Kellie. And the information in a SOC-2 audit would have to come from different resources in the organization.

Q. What is your understanding of what SOC-2 is?

A. SOC-2 is a certification for SaaS products that certain operational procedures and the product itself could do certain things.

Q. Okay. And you said that Ms. Pierce was tasked with making the trains run on time.

With whom was she working on the project?

A. The FedRAMP --

Q. Yes.

A. -- assessment?

Q. Yes.

A. I'm not aware of her working with anyone, and I would defer to her testimony on that, because we didn't want this to be a large, distracting project. We wanted it to be a cursory, back-of-the-envelope, how far are we?

Q. Did you think there was a serious possibility you were going to try to get FedRAMP certification at the time that this assessment was done?

A. The request would have been more from the business side. So, like, the sales side, because they want to sell more. And this is going

to help them in that effort. I believe there was a bias on the general and administrative team that this was a big effort and was going to be very distracting and we were not ready to engage on that.

Q. Why did you go through doing the assessment at all if the bias was against doing it?

A. We -- we wanted to understand, you know, how much work it would take. Even though we're biased doesn't mean you don't do it.

Q. Mm-hmm. Did you -- or did SolarWinds take any action as a result of the results of the FedRAMP assessment in terms of changing its internal cybersecurity practices?

A. Not that I recall.

Q. Was there any assessment based on the results of the FedRAMP assessment as to whether SolarWinds's cybersecurity practices were deficient in some way?

MR. TURNER: Objection to form.

A. No. This -- again, this was not a technical person reviewing our cybersecurity program, fact-finding and assessing the program.

Q. As -- prior to, like, March of 2018, was there a written secure development life cycle policy document at SolarWinds?

MR. TURNER: Objection to form and scope.

A. I don't know what you mean by "policy document," if it -- if it's this document itself. I don't even know if this describes full secure development or software development life cycle or if this was Steven Colquitt's program that was augmenting and evolving what we were already doing. But there are items in Confluence, for instance, prior to March of 2018 that illustrate software development life cycle activities, yes.

Q. I'm referring to secure development life cycle in particular as opposed to software development life cycle more generally.

And my question was as -- prior to March of 2018, was there a written secure development life cycle policy at SolarWinds as a document?

MR. TURNER: I object to form and scope.

A. There were items within Confluence, which is a wiki, W-I-K-I, that had procedures for

software development that would include certain of these activities, like code scanning.

Q. As you sit here today, there -- there seem to be a number of bullets under "Secure Development Life Cycle."

Are you aware of which, if any, of these were set forth in some SolarWinds internal document as a procedure prior to March of 2018?

MR. TURNER: Objection to form. And I'd just note we've produced the documents. You can read them yourself. The witness is not -- can't be expected to memorize everything he's seen.

A. Without seeing the documents, no. I don't have all that in my mind.

Q. So specifically with respect to security training, were there specified security training procedures within SolarWinds for -- with respect to a secure development life cycle prior to March of 2018?

MR. TURNER: Objection to form and scope.

A. I don't know the content of this document and what that's saying about security training, but I'd defer to Steven Colquitt's

testimony on what training was going on and Joe Kim's testimony on that.

Q. Okay. Turning your attention back to the cover email on the document, there's a statement from Ms. Pierce to Mr. Brown, Ms. Thornton, and I guess Phillips Akogun: "We have collected and redacted several security artifacts that would assist with customer questionnaires. We would like to review them with you before reviewing with legal."

Do you understand the purpose for which this document was being prepared as having something to do with customer questionnaires?

MR. TURNER: Objection to foundation and scope.

A. I don't specifically know without seeing the documents. But, again, in this time period, I hope we recognize we were getting a lot of questions from customers and we were trying to make sure that we were answering those questions appropriately, and this seems like a small part of that overall admission.

Q. Okay. What's a checkmarks report?

A. Checkmarks is a tool that I'll again defer to the technical resources and their

testimony precisely what it does, but part what have it does is code scanning.

Q. Okay. What's "BCP-DR"?

A. Where are you?

Q. The fourth -- the third bullet point. It says "BCP-DR is included in the policy table of contents."

What does BCP-DR mean?

MR. TURNER: Objection to scope and foundation.

A. I suspect that's business continuity plan and disaster recovery.

Q. Okay. It says "Pen test attestations have already been redacted and/or are shareable."

What's a pen test attestation?

MR. TURNER: Same objection.

A. I know what a penetration test is. I'm not sure precisely what the attestation is referred to here.

Q. Is it possible that in an NDA response to a questionnaire, a customer might ask to see your records of pen testing on some product and this would have something to do with that?

A. The first part is possible, that they would ask for a pen test of a product. The second

weren't written down at that point?
A. Certainly there were documentation that we were improving/enhancing prior to this as we were approaching -- you know, as we got through the GDPR process, for instance, as we were approaching being a public company. So there were lots of initiatives that were creating a need for documenting a lot of the activities that were going on through, you know, a couple-year period there.
Q. Okay. There are no specific policies you're aware of as you're sitting here based on your preparation that were being referred to as "needs improvement"?
A. No, I don't -- I don't know of a specific policy that would need improvement. No.
Q. Do you have any other further knowledge as to what projects had or had not been done for the items that were coded yellow?
A. Knowledge as to what had been done for those that are yellow?
Q. Yeah. What -- so yellow seems to imply somewhere between limited or nonexistent and strong program.
So do you have an understanding as to

what steps had been taken on the yellow as opposed to what had not yet been taken?
A. Not precisely, no.
Q. Okay.
MR. TODOR: New document.
(Whereupon, exhibit is received and marked Bliss Deposition Exhibit 13 for identification.)
THE REPORTER: Bliss 13 for identification.
BY MR. TODOR:
Q. Okay. And you've been presented with a document marked Bliss Exhibit 13. It has Bates SW-SEC00313351 through 3362. It appears to be a PowerPoint titled "Information Security - Risk Review October 2018."
Did you review this document in preparation for your deposition?
A. I did not.
Q. What was the function of a risk review in information security reportingwise within SolarWinds?
A. Again, I'm not sure -- similar to the one previously -- what the audience was for this presentation.

Q. Okay. Would you turn your attention to the last four pages of the document starting with Bates 3359?
A. Mm-hmm.
Q. And first slide states "A proactive security model - original plan and request from August 2017."
Are you with me there?
A. Mm-hmm.
Q. Do you understand this to be Mr. Brown's original plan and request from August 2017 for a proactive security model?
A. I'd defer to his testimony on that.
Q. Okay. Turning your attention to Bates 3361, there is a slide titled "Proactive security model - updated October 2018 with status."
Are you there?
A. Mm-hmm.
Q. And, again, there's some color coding in red, yellow, and green.
Do you know what the red, yellow, and green -- or does SolarWinds know what the red, yellow, and green are referring to here?
A. I do not without a legend.
Q. Okay. Is it reasonable to conclude that

it would be similar to what the red, yellow, and green meant in the information security incident review for September 2018 that we just looked at?
A. I'd probably defer to what Tim or Rani said about that.
Q. For the items under "Risk of Noninvestment," the first item -- and you can probably look to the one two pages before it if you want to see it in the black lettering. First bullet under "Risk of Noninvestment" coded in yellow states "Current state of security leaves us in a very vulnerable state for our critical assets. A compromise of those assets would damage our reputation and financially."
A. Mm-hmm.
Q. What is SolarWinds's understanding as to why this is coded yellow here?
A. Sorry.
My understanding of that statement, first, is that it was attached originally to a budget request being made. So as with any budget request, there's a certain amount of hyperbole that's introduced, but it's also identifying a risk, not a factual finding, of, look, if we're

investing, the static state today is going to leave us in a vulnerable state. And I hope every cyber person thinks that because if you stand still, you will be in a vulnerable state years from now as the macro is changing.

And I think that's -- the risk here that he's identifying is the macro's changing dramatically and we need to be investing in that.

Q. What is SolarWinds' understanding as to whether Mr. Brown was using hyperbole in this statement?

A. I would -- I would think he is using hyperbole in this statement.

Q. What's SolarWinds' basis for that conclusion?

A. It's natural human nature when you're in a budget request to be -- particularly in cyber, to be stating things of why you need budget. But, again, this isn't a fact of which he's being hyper -- hyperbolic about. This is a risk he's identifying.

Q. I direct your attention down to the fifth bullet. There's a statement: "Without training our employees will continue to be one of our biggest risks," which is coded in red.

big, it takes time to implement. And as you talk about training people, you're training people not just on the programs and the workflows, but on new tools you're introducing, for instance, and operationalizing that.

So you're doing that on a regular cadence. So when you bring in new developers or you acquire companies and you bring in developers en masse from acquisitions, you can get them to scale up the learning curve and standardize with the procedures he was recommending to augment our activities.

Q. Was this secure development training a budget request for an additional $30,000 approved?

A. I don't recall what the request was for or what was funded and whether it wasn't needed to be funded because, for instance, he might have been thinking about a tool, but we just encompassed it into our broader training tool, for instance, but I don't know the answer to that.

Q. You said in an earlier answer that this -- that these risks of noninvestment were not factual findings.

Is that what you said?

A. That first one in particular, yeah.

What is SolarWinds' understanding as to why that's coded in red?

A. I don't have recollections as to why this is a red.

Q. What was the status of SolarWinds' security training initiatives in October 2018 as they related to secure development training?

MR. TURNER: Objection to form and scope and foundation.

A. As it related to the Colquitt initiative?

Q. So I'm referring specifically -- there's a budget request slide here --

A. Mm-hmm.

Q. -- on the right that says "Secure Development Training, $30,000," and that is coded in red.

A. Mm-hmm.

Q. So what is SolarWinds' understanding as to why that is coded in red?

A. I don't have a specific recollection as to why that is coded in red, but as a reminder, Steven Colquitt had a program that he was introducing to up-level the secure development within the company. And as with a program that

That's an identified risk of in Tim's mind what a risk would be, much like we would say in risk factors, if we stayed still.

Q. So is the statement "Current state of security leaves us in a very vulnerable state for our critical assets" not a factual finding?

A. I do not think it is a factual finding.

Q. Why not?

A. I don't think that they believed there was any material issue with their cybersecurity program at this time.

Q. Why is saying "a very vulnerable state" not saying that there was a material issue with the cybersecurity program?

MR. TURNER: Okay. Object. You're asking him about Tim's state of mind. Tim has already testified that this was not a factual finding. You're asking about the company's position. He's told you the company's position.

Beyond that I'm -- I'm not sure what other information this witness has to provide.

MR. TODOR: That's what I'm

trying to find out.
A. I'd just go back to my hyperbole comments and he's identifying a risk and this is not a factual finding. And I'd defer to his testimony with respect to that as well.
Q. Turning your attention to the third bullet on 3361 under "Risk of Noninvestment." There's a statement: "We have had 22 reported security incidents this year. Reactive responses costs significantly more than being proactive." It appears to be coded red.
What's SolarWinds' understanding as to why that's coded red?
MR. TURNER: Objection to scope.
A. I don't recollect the reason for why that's red.
Q. I direct your attention --
A. I defer -- I defer to Tim's testimony.
Q. Okay. I direct your attention to the "Overall Budget Request" section to the section on "internal/external pen test." And there are figures that are coded yellow.
What's SolarWinds' understanding as to why that's coded yellow?

A. Again, I'd defer to Tim's testimony on why that's yellow.
Q. Did SolarWinds make a decision to prioritize internal as opposed to external pen testing at this time?
MR. TURNER: Objection to form, foundation, and scope.
A. I would defer to Tim if he testified on that, but I don't know.
Q. Okay.
MR. TODOR: Next document.
(Whereupon, exhibit is received and marked Bliss Deposition Exhibit 14 for identification.)
THE REPORTER: Bliss 14 for identification.
THE WITNESS: Thanks.
BY MR. TODOR:
Q. And you've been presented with a document marked as Bliss Exhibit 14 marked with Bates SW-SEC00001635 through 1652. Appears to be a PowerPoint, "SolarWinds Security and Compliance Program Quarterly, May 17, 2019."
So what was the purpose of security and compliance program quarterly documents within

SolarWinds?
A. I'd have to be reminded on the audience for this particular one.
Q. What is your understanding of who the audience was?
A. So -- so there are various reports of security compliance programs that would be perhaps more detailed within the IT organization that would get summarized as -- as we went to report to the executives, for instance. I'm not sure which one this exactly is. It looks to me like it's for presentation to the IT organization given the cover, but I didn't want to presume that without knowing.
Q. If you look at the second page, it looks like there are security and compliance initiatives as "legal, financial, product, federal, security, and information technology."
Does that suggest anything to you about who the audience would be?
A. No, not this slide. No.
Q. Okay. Is it likely it's someone fairly senior?
A. I don't know.
Q. Do you have any knowledge -- and you can

look at the page 1641 for security compliance initiatives listed for security.
Do you have any knowledge of the technical input that went into these?
A. Are you asking if I have knowledge as to the kind of diligence underneath these?
Q. Yeah. So, like,what would be the -- the workflow for coming up with that first item, "Secure Development Life Cycle, working with the engineering and development teams to continue to mature and adopt the SDL"?
How was that statement generated?
A. I don't know who authored it or generated it.
Q. Okay. Would it be a typical practice for the information security group to take the lead on developing the security and compliance initiatives for security?
MR. TURNER: Object to form.
A. Can you say that maybe slightly differently?
Q. Okay. So the secure development life cycle says "Working with the engineering and development teams..."
Who is working with the engineering and

"Moving towards zero trust model (where we loosely protect all and strongly protect those that can do material harm). Less requirements on VPN."

What is SolarWinds' understanding as to what the status of progress was towards zero trust model as of the date of this presentation in August 16th, 2019?

A. We -- we're always looking to improve and zero trust is another model that was around that we were looking to make sure that as we provisioned and monitored, we were doing it according to that model. So it's -- it's just simply an improvement upon the least privilege model that we were implementing at this time.

Q. Why does it say "Less requirements on VPN"?

A. I'm not sure and I'd have to defer to any testimony that discussed that. It's probably more of a technical issue than I know.

Q. I direct your attention to the "Security Category" section and to the last row there. It states "Authentication, Authorization and Identity Management," and the objective is "user identity, authentication and authorization are in place and

actively monitored across the company." And it says NIST maturity level is 1.

What is SolarWinds' understanding as to why the NIST maturity level was 1 for that item?

A. So, again, subjective determination. Generated a conversation in this venue in particular of ongoing activities. I mentioned Azure, A-Z-U-R-E, as one of those activities. And it refers again to standardization of the identity management across all of SolarWinds and its properties.

Q. What was SolarWinds' understanding of what steps needed to be taken to improve the NIST maturity level from 1 to a higher level as of this point?

A. The completion of a -- of projects that were in place, in particular Azure AD, and the rolling out of that tool and training behind that tool to the full organization is an example.

Q. Any other examples that you're aware of?

A. I'm not aware of this determination referring to more than that, but I would defer to any testimony that might highlight anything.

Q. I turn your attention to Bates 1523

within the document. And this is a slide marked "Financial: Enterprise Access Management (SOX compliance)."

What was the role for, I guess, the -- the financial review for enterprise access management at SolarWinds?

MR. TURNER: Objection to form.

A. What -- what do you mean by the process?

Q. So was it something that would be part of the SOX compliance audit?

MR. TURNER: Would -- would what be part of the --

MR. TODOR: Enterprise access management.

A. It would be part of the Sarbanes-Oxley initiative, yes.

Q. Okay. And I direct your attention to the description that states "Access management describes the management of individual identities, their authentication, authorization, roles, and privileges within the enterprise in order to minimize security risks associated the use of privileged and nonprivileged access." It

looks like there probably should have been a "with."

Was that an initiative at SolarWinds to improve on access management in the -- on around August 2019?

MR. TURNER: Object to form.

A. I think this was an attempt to describe what this project is.

Q. Okay.

A. Probably imperfect.

Q. Okay. And looking at the "Issues, Risks and Dependencies," category 1.1, it says "Concept of least privilege not followed as a best practice."

What was SolarWinds' basis for describing that as an issue, risk, or dependency?

A. I believe that's an identified risk. That could be the case, but I don't know -- I don't agree that least privilege was not followed, if that's your question, at this time period because there's ample evidence that it was.

Q. Okay. There are some timelines here, key milestones.

Do these relate to progress on the

concept of least privilege being followed as a best practice?
A. You -- you mean the key milestones --
Q. Yes.
A. -- status case?
Q. Yes.
A. So this is kind of a project template and the issues, risks, dependencies are kind of the risks or identified issues, but the least privilege one's a risk that this project is hoping to address. Right? So some of these milestones over here may or may not pertain directly to that identified category.
Q. So if I look at Phase 7 down there, it says "Finalize access SARF, implement SARF changes/exceptions."
A. Right.
Q. I think you might have spoken to this earlier.
What's SARF?
A. SARF is system access request form. So the SARF process predated the relevant period and it had evolved over time. So it was a somewhat manual process of distributing a form around to stakeholders that would have input as to what

access rights an individual -- an employee, for instance, being onboarded -- would need. And they would describe least privileged systems that they need access to. And they would require an approval process if there is a need for that role to have access to systems beyond what's described.
Q. Mm-hmm.
A. The changes we've made over time were to -- mostly to automate that more and more, and it roughly lines up with this time period when we were looking at doing more automated procedures around the SARF.
Q. Was there any finding within SolarWinds that SolarWinds' SARF processes presented a SOX compliance problem?
A. Nothing significant, but a SARF -- a manual process, whatever it is, and SARF included, had prone to isolated incidents such as a form not being filled out accurately or the access rights not being provisioned on a perfectly timely basis, but those were very isolated. The more you could automate that, the thought was you could reduce those isolated exceptions.
Q. Okay. And looking at the timeline for

this finalizing access SARF and "implement SARF changes/exceptions," it has a start of 12/2019 and finish of 2/2019. I'm guessing that might have meant 12/2018.
What was SolarWinds doing during that phase of the process if you know?
A. I don't recall specifically what was being done. I do know that the SARF form changed at some point roughly around this time period to reflect a more automated procedure.
Q. Okay. And then the eighth step there says "Internal audit, Holtzman audit, audit remediation."
What activities is that referring to with respect to "Enterprise access management (SOX compliance)"?
A. I don't recollect exactly what that's referring to.
Q. What would -- would audit remediation imply that there was some finding of a deficiency in the audit that needed to be corrected somehow?
A. A deficiency in the actual audit procedures?
Q. In the -- the audit found some

deficiency with respect to enterprise access management that had to be remediated somehow.
A. Not necessarily.
Q. Okay. Why? What else might it mean?
A. It could mean to the point there are events that were highlighted in user access reviews, for instance, that we would go remediate, as you suggested. It could also mean that the audit procedures, for instance, were pulling things from -- from, you know, wrong time periods, for instance. I don't know. But we were doing user access reviews, which is part of the audit procedures, identifying any user access exceptions and remediating those. So it could mean that.
Q. Okay.
MR. TODOR: Next.
(Whereupon, exhibit is received and marked Bliss Deposition Exhibit 16 for identification.)
THE REPORTER: Bliss 16 for identification.
BY MR. TODOR:
Q. You've been presented with a document marked as Exhibit 16. It appears to be -- has

confirm that without source.
Q. Okay. And I'll refer your attention to Bates 1587, the one that marked as the "SolarWinds scorecard."
And was SolarWinds's understanding as to the progress, if any, made with respect to the second half of 2020 improvement plan items that are listed first for "Identify" for "Increase SDL awareness and adoption" compared to the previous QRR that we reviewed?
A. That was Exhibit...
Q. This one was 18. Would have been -- this one is 20. It would have been 18.
A. Okay. So the key risks are the same, which is what I would expect. The improvement plan has some changes on it.
Q. And what -- was there any -- what -- what was the state of progress on those improvement plans according to SolarWinds' knowledge of this review compared to the prior ones we looked at?
MR. TURNER: I would just note there -- there are two prior pages that seem to go into greater detail on this. There are also a number of

second-half updates after the -- this slide as well.
BY MR. TODOR:
Q. I guess -- let me ask this way.
Do you have any reason -- does SolarWinds have any reason to believe that the descriptions of the projects and their update status as listed in this slide deck are inaccurate?
A. I'm not sure if they accurately or inaccurately project activities going on. You know, one obvious observation is the world pretty much blew up in this time right now, right? So this was COVID and our entire employee workforce was now at home. So, you know, this wasn't predicted earlier in 2020. And as any good team does, they would have to shift priorities to addressing that which was an impressive effort.
So I think that context is super critical to this entire assessment of 2020 and I trust there were some advances.
Q. Mm-hmm.
(Whereupon, exhibit is received and marked Bliss Deposition Exhibit 21 for identification.)

THE REPORTER: Bliss 21 for identification.
BY MR. TODOR:
Q. Okay. You've been marked -- presented a document marked Bliss 21. It has Bates SW-SEC00006628 through 664 -- 6628 through 6648. Appears to be a PowerPoint marked "SolarWinds PM Security Vulnerability and Incident Review, July 10, 2020."
What was the function of this document within SolarWinds?
MR. TURNER: Object to scope and foundation.
A. I'd have to defer to the testimony of Tim.
Q. Okay. Is -- to your understanding, is this a document Mr. Brown would have prepared?
MR. TURNER: Same objection.
A. I am not sure if Tim would prepare this, contribute to it, or not.
Q. I turn your attention to Bates 6635, and this is a slide marked "ITOM Core Highlights and Asks."
What does ITOM mean?
A. ITOM here refers to the business unit

that I previously referred to called Core-IT. It had a different nomenclature, but ITOM was this kind of preceding this.
Q. I direct your attention to under "Highlights." The fourth bullet there states: "Inconsistent internal security testing as part of product final security reviews don't always include web application testing before release."
What is SolarWinds' understanding as to the basis for that statement?
A. I'd have to defer to the testimony of somebody like Tim on this, but it's under "Highlights" with both Whitesource and checkmarks with green checkmarks next to them --
Q. Mm-hmm.
A. -- which my interpretation of this is this is an improvement on the overall program that you're looking at.
Q. Okay. And what are Whitesource -- what's Whitesource?
A. It's a -- it's a tool in the development life cycle. What precisely it does, I'd have to defer to Tim's testimony on.
Q. Okay. And I think you discussed checkmarks previously.

Is that --
A. I did.
Q. -- the same understanding as to what function it would have with respect to internal security testing as in your prior answer?
A. Yes.
Q. There's a -- the first bullet states "Customers continue to actively engage third-party penetration testers as part of their compliance efforts."
Does that -- what is SolarWinds' understanding as to why the customers would be engaging third-party penetration testers?
A. The industry at large was evolving around this time. And just like we were getting more questions, people were now engaging with penetration testers that they preferred or liked and we rely on those.
Q. Okay. Was this a statement that SolarWinds's penetration testing was inadequate?
A. No.
Q. What's the basis for that statement or that response?
A. My general experience with these customer inquiries is there are a number of

penetration tools that were out there and we used some of them and they were good. Customers would sometimes use a different tool and would not necessarily rely on what the company had done with their tool.
So that just created potential friction and, thus, create a risk in the sales process.
Q. Okay.
MR. TURNER: Jason, I think the question was, was the fact that customers were doing pen tests at all an indication SolarWinds' pen testing was inadequate?
THE WITNESS: The -- the answer to that is no, and it was more just this is part of customer activity of doing pen tests themselves just like we would on vendors.
BY MR. TODOR:
Q. Do you have any other understanding as to why that was listed as a -- a highlight in that section beyond what you've testified to so far?
A. No.
MR. TODOR: We are getting to Topic 8.d. We can either press on or

if you need to take a break, we can do that.
MR. TURNER: Up to you, Jason.
THE WITNESS: Let's take a quick break before my bladder blows up.
THE VIDEOGRAPHER: The time right now is 6:28 p.m. and we are off the record.
(Whereupon, a recess is taken.)
THE VIDEOGRAPHER: The time right now is 6:44 p.m. and we're back on the record.
BY MR. TODOR:
Q. Hello again, Mr. Bliss. I direct your attention to Topic 8.d of the deposition notice, which is "Internal audits relating to cybersecurity practices, including, but not limited to, audits of IT general controls, Sarbanes-Oxley audits, SOC Type 2 audits, and ISO 27001 audits," and then some Bates numbers.
We discussed SOX audits earlier.
Are you aware -- is SolarWinds aware of any other findings in SOX audits with respect to a deficiency with respect to access controls other than the one that we discussed in the March 2020

email and in the QRR?
A. I don't --
MR. TURNER: Objection to scope.
A. I don't recall any other than those isolated events that we looked at.
Q. Okay. And in audits of IT general controls, were there any findings of deficiencies with respect to access controls at SolarWinds --
MR. TURNER: Same objection.
Q. -- in the relevant time period?
A. I don't -- I mean, you the word "deficiency." I'd say there were exceptions to the overall access rights that were identified and remediated, none of which rose to the level of a significant deficiency, much less a material weakness, for instance.
So I hesitate to call it deficiency because it relates to an accounting term.
Q. Okay. With respect to SOC Type 2 audits, were there any findings of deficiencies with respect to access controls in the relevant time period?
A. I don't recall. Obviously, a SOC-2

majority products," I'm guessing it could be "of products."
What is SolarWinds' understanding for the basis for that statement?
A. I don't have any basis for that statement.
Q. Okay. The second sentence states "In addition, there is no governance in place to help provide consistency."
What is SolarWinds' understanding of the basis for that statement?
A. I -- SolarWinds doesn't believe there is a basis for this statement. We just pored through a number of large documents that suggest otherwise.
Q. And with respect in particular to the RMM and central and backup documents that are being referred to as "key MSP products" on the previous page, what is SolarWinds' understanding as to the design documentation for those products as relates to the issues discussed here?
MR. TURNER: Objection to form and scope.
A. I don't think that SolarWinds understands these authors and what they're trying

to communicate with this statement.
Q. Okay.
A. Because it -- the fact that design documentation is lacking, we know there's design documentation for products, so I don't know if he's -- what he's expecting. And I'm not sure he had a firm basis for that or not.
Q. Does SolarWinds have an understanding of what the governance that is being referred to in the -- the second sentence would be referring to?
A. No.
Q. Turn to the third sentence there. There's a statement "These are crucial for threat modeling and other security activities in SSDLC."
What is SolarWinds' understanding as to the basis for that statement?
A. I'm not sure of the precise basis of the statement. Again, we were doing threat modeling, so I'm not sure where he's getting his information to come to these conclusions.
Q. Was -- is it SolarWinds' understanding that SSDLC is referring to secure software development life cycle?

A. I'm not sure if Stas was referring to that specifically or the program. It's kind of unclear.
Q. Next statement is "This should be covered by architecture, as part of the SSDLC process being formed."
What is SolarWinds' understanding as to the basis for that statement?
A. I don't understand the basis for the statement or what he's referring to when he's precisely saying "the SSDLC process" in the statement.
Q. As of July 2019, was there a secure development life cycle process being formed for MSP products separate from that for the Core-IT?
A. I'm not aware of one.
Q. By "architecture," which group at SolarWinds is being referred to there to SolarWinds' knowledge?
A. Not -- I don't understand precisely which team he's referring to, but there is a group that's considered architects in engineering.
Q. I turn your attention to the next page of the document, Bates 6794. And I'll turn your attention to the heading "Risk assessment

(Identify)," and would ask you to look first at the first subheading there. Let me know when you're ready to discuss.
A. Okay.
Q. And the first subheading is "Asset vulnerabilities are identified and documented." The statement is "Each product seems to have its own ways of marking security issues that do not follow recently established SW standards."
What is SolarWinds' understanding for the basis for that statement?
A. I don't think we understand the basis of the statement and I'm not sure I understand what the statement is really saying.
Q. Next -- I'd ask you to read the next subheading and statement and let me know when you're ready to discuss.
A. Okay.
Q. And the statement "Currently, there is no formal process in place for reporting" -- the -- the heading is "Threat and vulnerability information is received from external sources." The first statement is "Currently, there is no formal process in place for reporting purposes."

What is SolarWinds' understanding for the basis for that statement?

A. I have no understanding for the basis of that statement because there was a process in place for reporting purposes.

Q. I direct your attention to the last sentence in that section. There's a statement, "A pre-requirement to have a policy to maintain proper third-party asset list, OS versions utilized, et cetera, to have data to work with."

What is SolarWinds' understanding for the basis for that statement?

A. SolarWinds doesn't understand what that statement is saying. It -- my guess is this may be an English-as-a-second-language author --

Q. Mm-hmm.

A. -- and I'm not sure I would apply such precision to much of these words, but I don't understand that last sentence.

Q. Okay. I direct your attention to the third subheading and ask you to review that and let me know when you're ready to discuss.

A. Okay.

Q. And the first statement, "No" -- the subheading is "Threats internal and external are

identified and documented." The statement "No threat modeling nor analysis is performed as part of any process (except MSP backup engineering)."

What is SolarWinds' understanding for the basis for that statement?

A. We have no knowledge of the basis for that statement, as we know threat modeling was done and analysis was being performed.

Q. Okay. Turn your attention to the fifth subheading. I'd ask you to help read that with you. Statement is "Threats, vulnerabilities, likelihoods and impacts are used to determine risk." The statement is "No coverage due to missing pre-requirements."

What is SolarWinds' understanding for the basis for that statement?

A. Again, I'm not sure SolarWinds understands what that statement is even saying, much less what the basis of that statement is.

Q. Does SolarWinds have an understanding as to whether threats, vulnerabilities, likelihoods, and impacts are used -- were used to determine risk for its MSP products as of July 2019?

MR. TURNER: Object to form.

A. I admit I'm not sure what likelihoods and impacts are here, but if it was identifying threats and identifying vulnerabilities and determining risk, yes, we were doing that.

Q. Okay. I turn your attention to Bates 6796 within the document and direct your attention to the I guess first main heading "Awareness and Training (protect)," and ask you to read that section and let me know when you're ready to discuss.

A. Just the "All users are informed and trained" part?

Q. Yes.

A. Okay. Okay.

Q. And the statement is -- the subheading is "All users are informed and trained." The statement is "There is no security awareness training as well there is no security training during the onboarding process."

What is SolarWinds' understanding for the basis of that statement?

A. Again, I do not know what the basis for that statement was as there was security training being done.

Q. There were a lot of I guess what would

appear to be alarming statements in here as to the types of security practices.

Did SolarWinds take any action in response to this document?

MR. TURNER: Object to the characterization.

A. I'm not sure whether there were specific actions taken, but the fact that I don't know these gentlemen's names suggests to me they were likely very junior members of the team that may not have full context or information as to what was going on and perhaps was putting together a document with very bad English that maybe they needed to deliver. But -- and as part of a smaller business unit of the company, I am not going to be alarmed by simply looking at this.

Q. Okay. Does SolarWinds know to whom this document was sent?

A. No.

Q. Does SolarWinds know whether any specific action items were taken as a result of any of the statements in the document?

A. No.

Q. Turning to Topic 8.f in the deposition

A. Well, there are many questions outside of what's here in the knowledge base. So legal would have a level of technical that I explained, but not necessarily to a depth of perhaps somebody in the Dev-Ops team, for instance, and would ask questions -- and that person might have answered the question to begin with -- but asked questions about the veracity of the information.

MR. TODOR: No further questions at this time.

MR. TURNER: Just briefly.

RECROSS-EXAMINATION

BY MR. TURNER:

Q. We talked about vetting these statements. This a password statement, okay, is a statement simply that complex passwords are required that use alpha and numeric characters. Was that done at SolarWinds?

A. Yes.

Q. It was done through Active Directory. That's your testimony, right?

A. Yes.

Q. Would Eric Quitugua needed to have spent significant time to vet that information?

A. No.

Q. Why?

A. Because it was obvious.

Q. Thank you.

MR. TURNER: No further questions.

MR. TODOR: No further questions at this time.

THE VIDEOGRAPHER: The time right now is 7:47 p.m. and we're off the record.

(Whereupon, the deposition was concluded at 7:47 p.m.)

STATE OF NEW YORK.)
) ss:
COUNTY OF NEW YORK)

I hereby certify that the witness in the foregoing deposition, JASON WALLACE BLISS, was by me duly sworn to testify to the truth, the whole truth and nothing but the truth, in the within-entitled cause; that said deposition was taken at the time and place herein named; and that the deposition is a true record of the witness's testimony as reported by me, a duly certified shorthand reporter and a disinterested person, and was thereafter transcribed into typewriting by computer.

I further certify that I am not interested in the outcome of the said action, nor connected with nor related to any of the parties in said action, nor to their respective counsel.

IN WITNESS WHEREOF, I have hereunto set my hand this 29th day of October 2014.

Reading and Signing was:

___ requested ___ waived _X_ not discussed

_____
BRIDGET LOMBARDOZZI, CSR, RMR, CRR

CERTIFICATE OF WITNESS

I, JASON WALLACE BLISS, do hereby declare under penalty of perjury that I have read the entire foregoing transcript of my deposition testimony, or the same has been read to me, and certify that it is a true, correct and complete transcript of my testimony given on October 16, 2024, save and except for changes and/or corrections, if any, as indicated by me on the attached Errata Sheet, with the understanding that I offer these changes and/or corrections as if still under oath.

_____ I have made corrections to my deposition.

_____ I have NOT made any changes to my deposition.

Signed: _____
JASON WALLACE BLISS 30(b)(6)

Dated this _____ day of _____ of 20____.

ERRATA SHEET
30(b)(6) Deposition of: JASON WALLACE BLISS
Date taken: OCTOBER 16, 2024
Case: SEC v. SOLARWINDS CORP., et al.
PAGE LINE
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
_____ _____ CHANGE: _____
REASON: _____
Signed_____
Dated_____

317

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE

Notice of Errata – Deposition of Jason Bliss (October 16, 2024)

I, the undersigned, do hereby declare that I have read the deposition transcript of Jason Bliss dated October 16, 2024 and that to the best of my knowledge, said testimony is true and accurate, with the exception of the following changes listed below:

Pages and Line(s)	Change		Reason
	From	To	
36:12	"externally, it was the initial"	"externally, the initial"	Clarification
36:14–15	"come in directly to information security group, but they would bring those"	"come in directly to the information security group, and they would bring those"	Clarification
38:14	MSP	MSPs	Typographical error
38:23	"refer to them as"	"refer to as"	Clarification
46:23–24	"VP security and architecture"	"VP of security and architecture"	Typographical error
60:11	"changes is kind of the answer"	"changes kind of the answer"	Typographical error

Pages and Line(s)	Change		Reason
	From	To	
64:9	log	blog	Typographical error
83:6	"between legal"	"and between legal"	Clarification
89:7–9	"but anything in this security statement with role-based access and authentication authorization is a very high level things"	"but anything in this security statement, with role-based access and authorization, are very high level things"	Clarification
94:23	"voice upon"	"voice on"	Clarification
99:13	responsible	responsibility	Typographical error
106:20–21	"I think it makes sense these are related exercise."	"I think it makes sense. These are related exercises."	Clarification
116:4	team	Tim	Typographical error
125:15	"as I know"	"as far as I know"	Typographical error
137:24	"That was"	"There was"	Clarification
179:11	"material of"	"material or"	Typographical error
208:2	"have it does"	"it does"	Typographical error
238:19	"had prone to isolated"	"is prone to isolated"	Clarification
289:4	"sparked in any of our minds"	"sparked concern in any of our minds"	Clarification

Pages and Line(s)	Change		Reason
	From	To	
297:21	"August of '24 (sic)"	"August of '18"	Clarification

I declare under penalty of perjury that the foregoing is true and correct.

Date: December 4.00, 2024 Signed: DocuSigned by: F604707628FC4BA... _____

Jason Bliss